Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Local Division Mannheim

UPC_CFI_636/2025
Procedural Order
of the Court of First Instance of the Unified Patent Court
issued on 25 July 2025
App_32933/2025

Applicant

Centripetal Limited
Galway Technology Centre, Mervue Business Park, 7XPF+6C Galway,
Ireland

represented by: Dr Ralph Nack, Dr Niclas Gajeck, and Ernesto Garzón Villada (lawyers), Noerr PartG mbB, Brienner Str. 28, 80333 Munich
and
Dr Frank Meyer-Wildhagen, Dr Martin Meggle-Freund, and Matthias Block (European Patent Attorneys),
MFG Patentanwälte PartG mbB, Amalienstraße 62, 80799 Munich

electronic address for service: ralph.nack@noerr.com

Defendant

Palo Alto Networks, Inc.
3000 Tannery Way, Santa Clara, 95054 CA, USA, with its branch office in Rosenheimer Straße 143c, 81671 Munich, Germany

represented by: Dr Henrik Lehment, Hogan Lovells International LLP, Dreischeibenhaus 1 - 40211 - Düsseldorf - DE

electronic address for service: upc-hub@hoganlovells.com

PATENT AT ISSUE: EP 3 281 580

PANEL/DIVISION: Local Division in Mannheim

DECIDING JUDGE: Prof. Dr. Peter Tochtermann acting as presiding judge and judge-rapporteur

LANGUAGE OF PROCEEDINGS: English

SUBJECT OF THE PROCEEDINGS: Application for Penalty Order

STATEMENT OF FACTS:

1. Applicant motioned for a saisie order before the CFI aiming at seizure and real-time monitoring of a full setup of the Form of Infringement offered by Defendant. In its application, Applicant applied to have the Defendant set up such a system to be monitored at its premises within a period of one month. The CFI LD Mannheim rejected the application for various reasons by order of 3 March 2025, amongst them a failure to submit sufficient facts why the Applicant believed to get hold of the network solution it wished to analyse with the help of an expert at the premises described in the application. Upon appeal the CoA (order of 28 May 2025, APL_13242/2025, UPC_CoA_239/2025) accepted the application in a modified version allowing the Applicant to carry out monitoring of Defendant's system at the premises contained in the application. The CFI thereafter issued the respective order upon referral back (order of 3 June 2025, amended by order of 9 July 2025 upon further application).

2. On 11 July 2025 Claimant executed the order and tried to monitor the Form of Infringement. However, it turned out that at the premises – a co-working space – there was only one sales person, which did not have any access to the layers of the system Applicant wanted to monitor. Counsel of Defendant, which had been called to come to the premises in accordance with the CFI order, which allowed the execution only after Defendant had been informed by the Applicant about its right to seek assistance of a legal representative of its choice to attend said inspection and allow Defendant a maximum of two hours to ensure the presence of such representative, refused to have the Defendant set up access rights from the US headquarters so as to grant the person at the Munich office the rights just for the purpose of the inspection so as to be able to provide the access sought by Applicant. The Applicant's outside counsel searched the entire office, but did not find any Next Generation Firewall, cloud computing servers, or any technical documentation. Applicant's counsel (not the bailiff or the expert) requested from the present staff member and the Defendant's counsel to somehow create a proprietary access to allegedly existing technical documentation stored outside the address named in the operating part of the Saisie Order and not accessible for the personnel present in this office. Neither the present staff member nor the Defendant's counsel were at the time able to create such proprietary access.

3. With the request lying before the court, Applicant requests as follows:

I. **Defendant is held in contempt of the Order of this Court dated 3 June 2025, ACT 8278/2025, CFI 142/2025 (hereinafter, "the Order") starting from 11 July 2025 for non-compliance with the requirements set by this Court in Items 3. c) and d) of the Order.**

II. **Defendant is ordered to pay to the Court a penalty in the amount of EUR 50.000,- per day for each day of non-compliance, commencing from 11 July 2025 as the first day of non-compliance with the Order.**

III. **This daily penalty shall be raised to EUR 100.000,- per day for each day of non-compliance with the Order occurring after the rendering of this order.**

IV. **This daily penalty shall be further raised to EUR 1.000.000,- per day for each day of non-compliance with the Order occurring after 20 days from the date of rendering of this order.**

V. **Defendant is ordered to report to Applicant any deletions of and/or changes to any technical documentation that is relevant to the measures for the preservation of evidence, ordered by the Court on 3 June 2025, which occurred on or after 11 July 2025.**

4. Applicant argues that drastic penalties had to be imposed as Defendant blatantly rejected complying with the obligation to provide the Court Expert the requested access to their systems and digitally available documentation.

5. Defendant requests to dismiss the request for enforcement. It argues Applicant chose the wrong premises (a sales office belonging to an affiliate of the Defendant) for its Saisie. There were no act of non-compliance by the Defendant. Claimant could have avoided this by simply looking at the company register of the affiliate of the Defendant. Had it done so, it would have realized that there most probably is no such system to be monitored available. Neither a NGFW hardware device (that was supposed to be monitored in real-time by the expert), nor any technical documentation had been available and the only persons present in the office was sales personnel without access to technical documentation. The entire Saisie Application of the Applicant were based on a fundamental misconception and misrepresentation about the office in Munich. The office were not a branch office of the Defendant (Palo Alto Networks, Inc., Santa Clara, USA), but the seat of Palo Alto Networks (Germany) GmbH, which – according to the German company register – only was involved in sales and marketing activities. Defendant argues that it had been in full compliance with the order. The Saisie Order did not contain any basis for enforcing against technical personnel located outside the office in Munich – or even outside the UPCA territory, such as in the United States. Even if one would accept such a duty, it would have been practically impossible to reach a competent person at 5:20 a.m. local time in the US.

GROUNDS FOR THE ORDER

6. Art. 60 (3) UPCA, R. 199 RoP and the rationale of R. 192.2(b) RoP demand that the scope of the inspection ordered is described in the court order as concrete as possible to guarantee that the interference with the rights of the Defendant is proportionate on the one hand and ensures the effective enforcement of the rights of the patent owner on the other hand

as demanded by Art. 7 of the Enforcement Directive (cf. Tilmann, Einheitspatent, Art. 60 para 61).

7. The premises to be inspected therefore have to be defined as precisely as possible in the order so as to further ensure that fundamental rights of the defendant according to Art. 8 ECHR, Art. 7 Charter of Fundamental Rights of the EU as well as national fundamental rights of the UPC-Contracting Member States are respected (cf. CoA, Order of 28 May 2025, APL_13242/2025, UPC_CoA_239/2025, paras. 19 et seqq.). As the premises to be inspected are detailed in the order, the inspection may not be extended to other locations, which are not included in the order, unless such locations are only adjacent locations, which have a close and obvious connection to the location detailed in the order. By limiting the local extent of the inspection the order also limits the extent of the inspection in general (cf. LD Paris 1 March 2024 – UPC_CFI_397/2023 para 59: "inspect products, devices, methods, premises or local situations in situ („descente sur les lieux")").

8. Accordingly, it may only be inspected what is found at the premises. The right to an inspection to the contrary does not extend to procuring items, which are not located at the premises, i.e. in case a patented machine cannot be found at the premises, the order for inspection does not oblige the defendant to bring the machine to the premises so as to allow the applicant to inspect it (cf. Böttcher in Kircher, Hdb. Europäischer Patentprozess, § 23 para. 268: no obligation to actively make contributions to the inspections but mere passive obligation to tolerate the inspection). Therefore, the defendant only has to cooperate actively in case his action is necessary to enable the Applicant's side to inspect the premises and the items which can be found at these premises as ordered. Typical examples are unlocking closed doors or entering a personal password so as to allow inspection of a computer workspace. However, the inspection of digital systems is limited to the digital system as it is present at the place of the inspection. If the IT system to be inspected is not accessible on the premises in question during the course of ordinary business activities carried out at these premises, as no staff member actively works with the system to be inspected and has no access rights to that system, the inspection does not require the defendant to increase access rights beyond the level required for ordinary daily business activities. Also, it does not require a defendant to bring hardware components to the premises, which are not there.

9. In consequence, in the present case, Defendant was under no obligation to increase the access rights of a mere sales person working at the premises detailed in the order to a level which would allow him to have access to the encrypted network security solution Claimant wished to monitor in real-time, if such increase of rights of the employee concerned is not necessary to have him carry out his duties required in his particular position as submitted by Defendant.

10. Furthermore, Defendant submitted that such increase of access rights can only be carried out by Palo Alto Inc., with its seat in Santa Clara, US, i.e outside the UPC-CMS and outside the scope of application of the REGULATION (EU) 2020/1783 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence). Claimant, however, described the place of the inspection to be a branch of Palo Alto Inc., which was not true, as the premises belong to a separate legal entity, Palo Alto Networks (Germany) GmbH. Therefore, the increase of user rights as requested by

Claimant would require Defendant to actively participate in the inspection beyond his duties under the order.

11. The CFI already rejected Claimant's initial request to have Defendant set up a system at his premises to be monitored in real-time exactly for that reason. Also the Court of Appeal did not accept Claimant's far-reaching request but ordered Defendant in a more limited form under ii. "to set up and monitor in real-time, at Palo Alto's German branch office located at Rosenheimer Straße 143c, 81671 Munich, Germany, Palo Alto's Network Security Solution, including in particular a NGFW hardware device with App-ID functionality, e.g. of the PA-1400, PA-5450 or PA-400 NGFW-series, that is connected to and operates with Palo Alto's ATP servers and has full access to the ATP software, to the extent necessary to provide the detailed description referred to in clause i.;" (cf. CoA ibid. para. 22) and continued to explain the understanding of that order as follows in para. 23:

> "This means that a court-appointed expert, his assistants and the bailiff will be allowed to enter the premises of Palo Alto's Munich branch office and search these for the relevant evidence, i.e. the relevant components of the system, digital evidence and documentation. The expert and his assistants may then examine the components of the system and monitor the functioning of a setup of the system at Palo Alto's premises. If necessary, they may create a setup of the system using the components available at that location. In addition, the expert, his assistants and the bailiff may make copies of the relevant documentation and digital evidence, including the data traffic within the monitored setup of the system. The bailiff will be authorized to take custody of the copies of the documentation and digital evidence. The expert and his assistants will have access to these copies in order to draw up his report describing the relevant features of the system. The expert may draft the report at a location of his choice."

and in para. 25:

> "It is sufficiently certain that at least part of Palo Alto's Network Security Solution and digital evidence and documentation is available at Rosenheimer Straße 143c, 81671 Munich, Germany, given that Palo Alto has a branch office there. An inspection of these premises is therefore justified. However, the Court of First Instance was correct in finding that Centripetal failed to demonstrate that a general inspection of the premises (request I.1.a) is necessary. The inspection may only be allowed to the extent necessary to monitor a setup of Palo Alto's Network Security Solution and to preserve digital evidence and documentation, as specified above in paragraph 22 under v. It will be at the discretion of the expert to what extent the inspection is necessary."

as continued in para 26:

> "The request for providing, seizing and monitoring Palo Alto's Network Security Solution (request I.1.b) must be granted in the more limited form specified in paragraph 22 under ii above. Firstly, at the oral hearing, Centripetal stated that the expert will be able to monitor Palo Alto's Network Security Solution and, if necessary, create a setup of Palo Alto's Network Security Solution with the available components, by himself without assistance from Palo Alto, if Palo Alto discloses the passwords, certificates, and decryption keys. Centripetal acknowledged that it is

therefore not necessary to order Palo Alto to provide the setup as requested under I.1.b of the application. Consequently, there is no need to decide whether there is a legal basis for compelling Palo Alto to provide such a setup. […]"

12. The order of the CoA, by which the CFI was bound after referral back, can only be construed so as to limit the inspection to the system actually being present at the premises of the order. There is no language which points into the direction of obliging Defendant to set up such a system in case it is not yet physically present with the necessary hardware components or with the access rights of the employees working at these premises. What Claimant sought to enforce during the inspection cannot be equated with entering a mere access code or password. Quite to the contrary, it would amount to actively setting up a system (including an access point with access rights) not being present at the premises, as had been clearly denied by both instances of the UPC. Such a request clearly goes beyond preserving evidence that is available at the premises to be inspected.

13. The conduct of Defendant can therefore not constitute a breach of the order so that no penalties are to be imposed. Before this background, Claimant's further request under item V. for reporting any deletions and/or changes also had to be rejected.

ORDER

1. The request to impose a penalty payment upon Defendant and to order Defendant to report to Applicant any deletions of and/or changes to any technical documentation that is relevant to the measures for the preservation of evidence of 15 July 2025 is rejected.

2. Claimant bears the costs of the enforcement proceedings.

Issued in Mannheim on 25 July 2025

NAME AND SIGNATURE

Peter Michael Dr. Tochtermann

Digital unterschrieben von Peter Michael Dr. Tochtermann
Datum: 2025.07.25 13:00:45 +02'00'

Prof. Dr. Peter Tochtermann
Acting as judge-rapporteur